A7 cncld.

57. (New) The method of Claim 55, wherein the action is creating an incident from a result.

58. (New) The method of Claim 49, further comprising applying additional scope criteria to a plurality of results.

59. (New) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 49.

REMARKS

Applicant has amended Claims 1, 3, 4, 16, 17, 20-22, 25, and 27-29 added new Claims 31 through 59. Claims 1 through 59 are now pending in the present application. The independent claims are Claims 1, 16, 27, 34 and 49.

If the Examiner believes that there are any issues that can be resolved by a telephone conference, or that there are any informalities that can be corrected by an Examiner's amendment, a telephone call to the undersigned at (404) 572-4600 to discuss same is respectfully requested.

Respectfully submitted,

Robert T. Neufeld
Reg. No. P-48,394

King & Spalding
45th Floor
191 Peachtree Street, N.E.
Atlanta, Georgia 30303
404.572.4600
K&S Docket: 05456.105005

Version with markings to show changes made

1. (Amended) A computer-implemented method for gathering security event data and rendering result data in a manageable format comprising the steps of:

creating scope criteria for analyzing security event data;

collecting the security event data from a plurality of security devices located at a first location;

storing the collected security event data at a second location; and

analyzing the collected security event data with the scope criteria to produce result data, the result data accessible by a plurality of clients.[; and

rendering the result data in a manageable format for the plurality of clients.]

3. (Amended) The method of Claim 1, wherein the first location is a distributed computing environment and the second location is a database server.

4. (Amended) The method of Claim 1, wherein [the second location is a database server] collecting the security event data comprises

generating security event data from a sensor;

sending the security event data from the sensor to a collector; and

converting the event data to a common format.

16. (Amended) A method for managing security event data collected from a plurality of security devices in a distributed computing environment comprising the steps of:

creating scope criteria for filtering security event data;

[collecting] generating security event data from a plurality of security devices located at a first location;

collecting security event data at a second location;

[storing the collected security event data at a second location;] and

applying the scope criteria to the [collected] security event data at a third location to produce a result, the result accessible by a plurality of clients coupled to a server.

17. (Amended) The method of Claim 16, further comprising rendering the result in a rendering for output to a client.

20. (Amended) The method of Claim 16, wherein the third location is an application server coupled to the [result is accessible by a] plurality of clients [coupled to a distributed computing environment].

21. (Amended) The method of Claim 16, further comprising storing one or more of the scope criteria, the security event data, and the result in a database.

22. (Amended) The method of Claim 16, [wherein in response to producing a result, an action is executed] further comprising executing an action at the server in response to producing the result.

25. (Amended) The method of Claim 16, further comprising applying additional scope criteria to a plurality of results.

27. (Amended) A computer-implemented system for managing security event data collected from a plurality of security devices comprising:

a plurality of security devices operable for generating security event data;

[a database server coupled to the security devices, the database server operable for collecting security event data from the security devices;

an application server coupled to the database server, the application server operable for analyzing the security event data; and]

an event manager coupled to the security devices, the event manager operable for collecting security event data from the security devices and analyzing the security event data; and

a client coupled to the event manager [application server, the client] operable to perform an action [for receiving a rendering of the] in response to receiving analyzed security event data from the event manager.

28. (Amended) The system of Claim 27, wherein the event manager comprises a database server [is further] operable for storing the collected security event data and the analyzed security event data.

29. (Amended) The system of Claim 27, wherein the event manager comprises an application server [is further] operable for creating an incident from the security event data for preparing a response.